CVE-2021-32032

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-32032
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-21 04:15:00 UTC
Updated	2021-05-27 22:33:00 UTC
Description	In Trusted Firmware-M through 1.3.0, cleaning up the memory allocated for a multi-part cryptographic operation (in the ever

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linaro	Trusted Firmware-m	All	All	All	All

References

Reference
crypto_multi_part_ops_abort_fail.rst « security_advisories « security « docs - trusted-firmware-m.git - Trusted Firmware for M profile Arm CPU
Trusted Firmware - Open Source Secure Software - Trusted Firmware
trusted-firmware-m.git - Trusted Firmware for M profile Arm CPUs
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report